特　許　協　力　条　約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　Ｍ０３－Ｎ－０８４ＣＴ１	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０３／１０１８６	国際出願日 （日.月.年）　０８．０８．２００３	優先日 （日.月.年）　０８．０８．２００２
国際特許分類（ＩＰＣ） Ｉｎｔ．Ｃｌ⁷　Ｇ０９Ｃ　１／００，　Ｈ０４Ｌ　９／０６		
出願人（氏名又は名称） 松下電器産業株式会社		

１．この報告書は、ＰＣＴ３５条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

２．この国際予備審査報告は、この表紙を含めて全部で　３　ページからなる。

３．この報告には次の附属物件も添付されている。

a ☒ 附属書類は全部で　１３　ページである。

☒ 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第６０７号参照）

☐ 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b ☐ 電子媒体は全部で＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、コンピュータ読み取り可能な形式による配列表又は配列表に関連するテーブルを含む。（実施細則第８０２号参照）

４．この国際予備審査報告は、次の内容を含む。

☒ 第Ｉ欄　国際予備審査報告の基礎
☐ 第Ⅱ欄　優先権
☐ 第Ⅲ欄　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
☐ 第Ⅳ欄　発明の単一性の欠如
☒ 第Ⅴ欄　ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
☐ 第Ⅵ欄　ある種の引用文献
☐ 第Ⅶ欄　国際出願の不備
☐ 第Ⅷ欄　国際出願に対する意見

国際予備審査の請求書を受理した日 １４．０１．２００４	国際予備審査報告を作成した日 ０８．０９．２００４	
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 石田　信行 電話番号　０３－３５８１－１１０１　内線　３５９８	5M　９４６９

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００４年１月）

特許性に関する国際予備報告

国際出願番号 ＰＣＴ／ＪＰ０３／１０１８６

第Ⅰ欄　報告の基礎

1．この国際予備審査報告は、下記に示す場合を除くほか、国際出願の言語を基礎とした。

☐ この報告は、＿＿＿＿＿＿ 語による翻訳文を基礎とした。
それは、次の目的で提出された翻訳文の言語である。
- ☐ ＰＣＴ規則12.3及び23.1(b)にいう国際調査
- ☐ ＰＣＴ規則12.4にいう国際公開
- ☐ ＰＣＴ規則55.2又は55.3にいう国際予備審査

2．この報告は下記の出願書類を基礎とした。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☒ 明細書
第 １－２７ ページ、 出願時に提出されたもの
第 ＿＿＿＿ ページ*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ ページ*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☒ 請求の範囲
第 ２，３，１２，１７－２０ 項、 出願時に提出されたもの
第 ＿＿＿＿ 項*、 ＰＣＴ１９条の規定に基づき補正されたもの
第 １，５－１１，１３，１５ 項*、 １６．０６．２００４ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ 項*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☒ 図面
第 １－６ ページ~~／図~~、 出願時に提出されたもの
第 ＿＿＿＿ ページ／図*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿ ページ／図*、 ＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

3．☒ 補正により、下記の書類が削除された。

☐ 明細書 第 ＿＿＿＿ ページ
☒ 請求の範囲 第 ４，１４，１６ 項
☐ 図面 第 ＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること） ＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること） ＿＿＿＿

4．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)）

☐ 明細書 第 ＿＿＿＿ ページ
☐ 請求の範囲 第 ＿＿＿＿ 項
☐ 図面 第 ＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること） ＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること） ＿＿＿＿

＊ ４．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／１０１８６

第Ｖ欄　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（N）	請求の範囲	１－３，５－１３，１５，１７－２０	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲	１－３，５－１３，１５，１７	有
	請求の範囲	１８－２０	無
産業上の利用可能性（ＩＡ）	請求の範囲	１－３，５－１３，１５，１７－２０	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

文献１：ＪＰ ２０００－７５７８５ Ａ（富士通株式会社），２０００．０３．１４
文献２：ＪＰ ７－２６１６６２ Ａ（富士通株式会社），１９９５．１０．１３
文献３：ＪＰ １０－２１５２４４ Ａ（ソニー株式会社），１９９８．０８．１１

請求の範囲１８－２０に係る発明は、国際調査報告で引用した文献１又は文献２と、文献３とにより進歩性を有しない。
文献１又は文献２には、ＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うことができるように構成された共用処理ブロックを具備する暗号化復号化装置の暗号化復号化方法が記載されており、該文献１又は文献２に記載された暗号化復号化方法の入力されるデータに、文献３の第６図，【００５２】－【００５９】段落に記載されているような、ＭＡＣ構造のヘッダに含まれる暗号化に関する制御ビットにより暗号化及び復号化の制御を行う構成を用いて、入力されるデータに応じてＣＢＣモード或いはＣＦＢモードを共用処理ブロックにおいて選択制御する構成とすることは、当業者にとって容易である。

請求の範囲１－３，５－１３，１５，１７に係る発明は、国際調査報告に記載されたいずれの文献にも記載されておらず、かつ当業者にとって自明なものでもない。

請求の範囲

1．（補正後） 暗号化データ又は暗号化すべきデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

入力された鍵データを用いたＥＣＢ（electronic code book）処理を行うことによって、ＣＢＣ（cipher block chaining）モード及びＣＦＢ（cipher feedback）モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで、前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、

前記処理ブロック入力データ、及び前記暗号処理データを入力とし、それぞれを遅延させて出力する遅延器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延器が出力する遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、

前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果として出力する第４のセレクタとを有するものであり、

前記ＥＣＢ処理器は、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

暗号化復号化装置。

２．　請求項１に記載の暗号化復号化装置において、

前記データ構造解析ブロックは、

前記暗号化データにおけるヘッダの解析を行い、前記ヘッダの情報に基づいて前記暗号化データからＭＡＣ（media access control）構造を抜き出し、前記ＭＡＣ構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該暗号化データが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に関する情報を前記制御用データとして出力するとともに、前記ＭＡＣ構造デ

ータから前記拡張ヘッダを除去して前記処理ブロック入力データとして出力するものである

ことを特徴とする暗号化復号化装置。

３．　請求項１に記載の暗号化復号化装置において、

前記データ制御ブロックは、

前記制御用データに従って、前記処理ブロック入力データをＣＢＣモード、及びＣＦＢモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示す信号を前記モード選択信号として出力するものである

ことを特徴とする暗号化復号化装置。

４．（削除）

５．（補正後） 請求項１に記載の暗号化復号化装置において、

前記ビットマスク器は、

前記モード選択信号が５６ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとして出力するものである

ことを特徴とする暗号化復号化装置。

６．（補正後） 請求項１に記載の暗号化復号化装置において、

前記第１のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前

記処理ブロック入力データを選択して出力し、その他の場合には、前記暗号処理データを選択して出力するものである
ことを特徴とする暗号化復号化装置。

７．（補正後） 請求項１に記載の暗号化復号化装置において、
前記第２のセレクタは、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択して出力し、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力し、
前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択して出力し、
前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力するものである
ことを特徴とする暗号化復号化装置。

８．（補正後） 請求項１に記載の暗号化復号化装置において、
前記第３のセレクタは、
前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であ

って、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

９．（補正後）　請求項１に記載の暗号化復号化装置において、

前記第４のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合には、前記排他的論理和演算器の出力を選択して出力するものである

ことを特徴とする暗号化復号化装置。

１０．（補正後）　請求項１に記載の暗号化復号化装置において、

前記ＥＣＢ処理器は、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合には、暗号化処理を行い、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、復号化処理を行い、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、暗号化処理を行うものである

ことを特徴とする暗号化復号化装置。

１１．（補正後）　暗号化データ又は暗号化すべきデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで、前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックと、

暗号化データ又は前記共用処理ブロックの出力を選択し、前記データ構造解析ブロックに出力する第１の入力セレクタと、

暗号化すべきデータ又は前記共用処理ブロックの出力を選択し、前記データ構

造解析ブロックに出力する第２の入力セレクタと、

所定の値又は前記共用処理ブロックの出力を選択し、出力する出力セレクタとを備え、

前記暗号化データ又は前記暗号化すべきデータに対して前記共用処理ブロックにおける処理が所定の回数行われると、前記出力セレクタが前記共用処理ブロックの出力を選択するように構成されている

ことを特徴とする暗号化復号化装置。

１２．　請求項１１に記載の暗号化復号化装置において、

前記所定の回数は、３回である

ことを特徴とする暗号化復号化装置。

１３．（補正後） 暗号化すべきデータを受け取り、そのデータ構造の解析を行って、制御用データを求めて出力するとともに、前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで暗号化を行い、得られた暗号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、

前記暗号処理データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、

前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算

器の出力のうちのいずれかを選択して、前記暗号化結果として出力する第４のセレクタとを有するものであり、

前記ＥＣＢ処理器は、

前記ＥＣＢ処理として暗号化処理を前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする暗号化装置。

１４．（削除）

１５．（補正後） 暗号化データを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで復号化を行い、得られた復号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記処理ブロック入力データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタ

データ、及び前記遅延器が出力する遅延した処理ブロック入力データのうちのいずれかを選択して出力する第２のセレクタと、

前記暗号処理データと前記第２のセレクタの出力との排他的論理和を求めて、前記復号化結果として出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器とを有するものであり、

前記ＥＣＢ処理器は、

前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする復号化装置。

１６．（削除）

１７．　受信した信号をデータに変換して出力するダウンストリームＰＨＹ部と、

前記データからダウンストリームデータ及び鍵データを分離して出力するダウンストリームデータ処理部と、

前記鍵データを用いて前記ダウンストリームデータを復号化して出力する第１の暗号化復号化装置と、